Does healthgrid present specific risks with regard to data protection ?

Herveg, Jean

Published in:
From genes to personalized healthCare : grid solutions for the life sciences

Publication date:
2007

Document Version
Publisher's PDF, also known as Version of record

From Genes to Personalized HealthCare: Grid Solutions for the Life Sciences
N. Jacq et al. (Eds.)
IOS Press, 2007

Does HealthGrid Present Specific Risks With Regard To Data Protection?

Jean HERVEG
Centre de Recherches Informatique et Droit, Faculté de Droit, FUNDP

Abstract. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data manages the risks in the processing of personal data in four steps. It provides notably that data processing presenting specific risks must be subject to prior checking beforehand. The paper investigates the theory of risks in Directive 95/46/EC, together with the criteria allowing to recognize those specific risks. Finally, the paper describes the consequences of such specific risks on the data processing.

Keywords. Processing of Personal Data – Specific Risks – European Law – HealthGRID

INTRODUCTION

The introduction of GRID technologies in healthcare arouses numerous legal questions [1]. Among these, one is to know whether the use of HealthGRID technologies could induce specific risks to the rights and freedoms of the data subject concerned by the underlying processing of personal data. Indeed, European Directive 95/46/EC imposes the prior checking of personal data processing presenting such specific risks. This legal issue is relatively important but should be serenely debated. This contribution aims to identify the criteria allowing to recognize these specific risks when using GRID technologies in healthcare.

1. The "Theory of Risks" in Directive 95/46/EC

European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [2] pursues a double objective when harmonizing the national legislations of the European Member States. It aims to allow for the free movement of personal data, asserted as necessary to the creation and the operating of the Common Market [3], and to ensure the respect of the rights and freedoms of the natural persons (individuals) concerned by the personal data [4]. The natural persons' rights and freedoms include their right to control in some way their personal data.

In order to remove the obstacles to the free movement of personal data in the Common Market, it is of prime importance to harmonize national legislations, so that all Member States offer an equal but high level of protection towards the rights and freedoms of the

persons regarding the processing of their personal data [5]. After such harmonization, the Member States may not prevent anymore the free movement of personal data for reasons relative to the protection of natural persons' rights and freedoms, these including the right to respect for private life. As the harmonization is limited in its material scope, the Member States may restrict the free movement of personal data for other reasons than those relative to the protection of natural persons' rights and freedoms [6] – without prejudicing the application of articles 95.8 and 95.10 of the Treaty creating the European Community or of any other rules opposing any restriction to the free movement of personal data within Member States or the Common Market.

In order to establish this legal framework shared by all European Member States (although relatively incomplete in a sense) regarding the processing of personal data, in the limits of its legal scope, the Directive results from a quantitative and qualitative assessment of the risks which the personal data processing may cause to the data subjects' rights and freedoms. This assessment has been realized to all levels of the Directive's scope. In this measure, the Directive determines its material scope (cf. Chapter One of the Directive) [7]. It focuses only on situations which require some protection. The latter implies to estimate the risks for the data subjects' rights and freedoms. For example, the Directive only applies to the completely or partially automated processing [8] of personal data [9] and to the non-automated processing of personal data figuring or aiming to figure in a filing system [10]. However, the Directive does not apply to the processing of personal data carried out by a natural person for exclusively personal or domestic reasons [11]. Furthermore, the Directive provides the general conditions for the lawfulness of the personal data processing (cf. Chapter Two of the Directive). It requires the existence of judicial remedies for the protection of personal data and creates a special liability upon the data controller, without omitting the question of sanctions in case of infringement of certain rules (cf. Chapter Three of the Directive). The Directive also rules the transfer of personal data outside the European Union (cf. Chapter Four of the Directive). Finally, the Directive addresses the question of the Codes of Conduct (cf. Chapter Five of the Directive) and establishes special institutions and bodies, such as the national supervisory authorities, the Working Group on the protection of individuals with regard to the processing of personal data (cf. Chapter Six of the Directive) and the Committee composed of the Member State Representatives concerning community implementing measures (Committee 31) (cf. Chapter Seven of the Directive).

Considered in a global approach, Directive 95/46/EC manages the risks presented by the processing of personal data by means of four steps [12]. In a first step, the Directive poses the legal framework applicable to any processing of personal data (including sensitive data [13]). In a second step, the Directive provides special rules to legitimate the processing of sensitive data. It goes without saying that the legal framework developed in the first step applies in addition to the processing of sensitive data. In a third step, the Directive imposes special rules to the processing of personal data presenting specific risks to the data subjects' rights and freedoms. This third approach must also be added to the two previous ones. It is not exclusive of their application for the rest of the data processing. In the fourth and last step, the Directive rules the transfers of personal data outside the European Union.

2. The Management of "Ordinary" Risk in the Processing of Personal Data

The risk management for the data subjects' rights and freedoms relies on a relatively simple principle: The risk does not depend on the informational content of the personal data but on the context in which they will be used [14]. In other words, the risk is linked to the purpose pursued by the processing of personal data. Therefore, the potential or real threat from the processing of personal data has to be assessed with regard to the purpose pursued by the data controller. There lies the reason why personal data are any information relative to an identified or identifiable natural person and not only information susceptible to reveal the intimacy of data subjects. Hence, all information, including the more common ones such as a phone number or a number plate, are personal data as long as they are related to an identified or (reasonably) identifiable natural person because the use of this kind of information may expose data subjects to some risks of infringement of their rights and freedoms, including their right to control in some extent the use of their personal data, with no regard to any specific informational content of the personal data. The aim of the Directive (the management of the risks presented by any use of information relative to identified or identifiable natural persons) explains for the definition of personal data.

3. The Management of "Special Risks" in the Processing of Personal Data

However, the principle relative to the risk management in the processing of personal data is slightly though not completely different with respect to the processing of "sensitive" data, the latter including medical data. Indeed, it is of common knowledge that the informational content of sensitive data is already capable to expose data subjects to some risks of infringement of their rights and freedoms in addition to the risk resulting from the purpose of their processing. In other words, any operation realized upon sensitive data inevitably exposes data subjects to risks of infringement of their rights and freedoms [14]. That is the reason why "sensitive" data require a special protection which has to take into account their informational content as well as the purpose of their processing.

Accordingly, the Directive bans the processing of "sensitive" data [15] because "data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed" [16]. Put otherwise, this ban represents the special protection adopted by the Directive for "sensitive" data, including medical data. Being prohibited, the processing of "sensitive" data is no more susceptible to present any risk for the data subjects' rights and freedoms. Somehow, this policy aims to minimize the risks presented by the processing of "sensitive" data.

Nevertheless, the Directive provides a number of cases in which the prohibition to process "sensitive" data does not apply [19]. In these cases, the legitimacy of the processing of "sensitive" data (their admissibility) is presumed. Indeed, these situations are of nature to justify derogation to the ban to process "sensitive" data without prejudice to the other rules applicable to the processing of personal data. Noteworthy, these exceptions to the prohibition to process "sensitive" data have to be strictly interpreted. Beyond these exceptions, the processing of "sensitive" data is not allowed.

In each of these exceptions, the risk presented by the processing of "sensitive" data is presumed to be adequately under control. It must be immediately stressed that these exceptions do not imply an absence of risk, but balance the interests in presence. This requires assessing the risks for the data subjects' rights and freedoms in order to reasonably appreciate the admissibility of the processing of "sensitive" data [19].

4. The Management of "Specific Risks" in the Processing of Personal Data

The Directive fixes the legal framework applicable in all Member States to the processing of personal data and provides special rules to legitimate the processing of "sensitive" data. Yet, the Directive considers the situation in which, without prejudice to this double approach, some processing of personal data may present some specific risks to the data subjects' rights and freedoms [17].

In 1995, the Directive has indicated that, regarding any processing of personal data in the society, the cases presenting such specific risks should not be very common [18]. More than ten years later and having in mind the vertiginous evolution of the new information and communication technologies, it is not clear that such statement be still valid. By contrast, the number of data processing presenting such specific risks seems nowadays quite significant, especially in healthcare. Indeed, since 1995 the technological evolutions have notably permitted the creation of huge telematic networks linking substantial medical databases and the creation of genetic databases in national or European or worldwide telematic networks. Should we consider that these evolutions have increased the number of data processing presenting specific risks for the data subjects' rights and freedoms?

The Directive provides that the specific risks result from the nature of the data processing, from its range or from its purposes [17]. For example, the Directive cites purposes aiming to exclude persons from the benefit of a right, a service or a contract. These specific risks may also arise from the specific use of a new technology [17]. The latter reminds inevitably the introduction of GRID technologies in healthcare.

Traditionally, the processing of personal data presenting specific risks are those pursued by public authorities and concerning the population (as a whole or in part) or those concerning medical data [20]. Genetic databases and telematic networks in healthcare are further examples of data processing susceptible to present specific risks to the data subjects' rights and freedoms. One should pay attention to the person of the data controller [21], to the sensitivity of the processed data, to the purposes of the data processing, to the range of the data processing, to the categories of data subjects and to the respect of their rights, keeping in mind the transfer of the personal data outside Europe. In short, one should beware anything that could create specific risks to the data subjects' rights and freedoms. But any processing of sensitive data does not necessarily present specific risks and the processing of "ordinary" personal data should not be a priori excluded as it may also present specific risks to the data subjects' rights and freedoms.

Regarding the development of the telematic networks in healthcare, the specific risks result primarily from the fact that patients' data may be processed for multiple purposes. This raises the question whether it is permissible to process medical data for multiple purposes. This also raises the issue of the prior determination of the precise

and real purposes of the data processing. In addition appears the question of further data processing. Indeed, the actual trend aims to not determine anymore on a prior and precise way the purposes of the data processing, but to organize an entire information system combined with a security system in which the data processing purposes will be determined later. Put differently, we witness today the creation of information system with two levels. First, the infrastructure of the information system is created, implying in some extent the collection and the processing of personal data in a virtual complex (notably to identify the actors of the information system – mainly the patients and the health practitioners). Only then, the purposes permitted by the infrastructure are determined, forgetting that these purposes rely on an initial data processing (the creation of the first level of the information system (its infrastructure)). Doing so, the creation of the first level of the information system does not seem to constitute such a risk to the data subjects' rights and freedoms even when this first level is at the origin of the risks. But both the first (the creation of the infrastructure or the network) and further data processing permitted by the infrastructure of the information system have to be assessed. And if the security level helps to assess the risks induced by the data processing, it does not prevent to take into account the other criteria's to legitimate the data processing (for both levels of the information system), especially when the processing concerns sensitive data such as medical data or genetic data.

These new information systems are part of a structural policy aiming at building telematic networks in healthcare. They also indicate the transition from a vertical conception of eHealth to a new conception which is, in a first step, abstract, horizontal and transversal (the infrastructure of the information system) and which, in a second step, becomes vertical and real (the applications - eHealth products and services - using the infrastructure). The mere existence of these new telematic infrastructures in healthcare enables to share scientific databases but implies the identification of the practitioners and patients through special registries, etc. Eventually, these telematic networks will deeply modify the organisation of the public health systems and all actors in healthcare will be concerned and involved: practitioners, patients, institutions and bodies in healthcare and social security, medical laboratories, etc.

But once again, these new information systems differ in their permanency, irrespective of their future applications. Hence, the opportunity to create these infrastructures is no more evaluated regarding their precise and real purposes. Their opportunity is assessed in an abstract way with respect to some categories of purposes whose precise and real content will be determined later. This constitutes a deep change in the required precision and reality to evaluate the purposes pursued by the creation of the telematic infrastructure and its future exploitation.

These new information systems with multiple levels and purposes pose problems regarding the fairness of the data processing since the latter requires to respect the precise and real purposes announced at the beginning of the data processing. It also poses problems with respect to the duty to properly inform the data subject. Indeed, the multiple ramifications of the information system are not transparent, regarding both the technical level as well as the purposes of the data processing ("black box" issue).

However, it must be said that the new information and communication technologies are able to address properly all these issues.

5. Consequences of the presence of « Specific Risks » in the Processing of Personal Data

Member States have a duty to identify the processing of personal data likely to present specific risks to the data subjects' rights and freedoms and to take appropriate measures to ensure the prior checking of the processing of personal data before their starting [22].

The fact that medical data are already subject to special rules due to their sensitive nature does not exclude them from the scope of additional rules relative to data processing presenting specific risks. In other words, the processing of medical data presenting specific risks for the data subjects' rights and freedoms has to be checked prior its beginning. However, any medical data processing does not automatically present specific risks. And processing of "ordinary" personal data may also arouse specific risks.

The prior checking of data processing presenting specific risks may occur in four different ways.

Firstly, the prior checking may be carried out by the national supervisory authority following receipt of the notification from the data controller [23]. The national supervisory authority may, according to the applicable national law, issue an opinion or authorize the data processing [24].

Secondly, the prior checking may be carried out by the data protection official [26]. In case of doubt the latter has to consult the national supervisory authority [23]. With respect to this, the Directive indicates that the data protection official will proceed in cooperation with the national supervisory authority [24].

Thirdly, the Directive provides that Member States may carry out the prior checking in the context of the preparation of a measure of the national parliament, which defines the nature of the data processing and lies down appropriate safeguards [25].

Fourthly, Member States may also carry out to this prior checking in the context of the preparation of a measure based on a legislative measure, which defines the nature of the data processing and lies down appropriate safeguards [25].

6. "Specific Risks" in the Processing of Personal Data and the use of HealthGRID technologies

It is now possible to know whether the use of HealthGRID technologies may induce "specific risks" with regard to data protection. This question is exclusively focused on the use of such technologies and not on the outlines of its implementation project. What could lead to the conclusion that the use of HealthGRID technologies may induce such specific risks?

a. The HealthGRID technologies phenomenal storage capacities are of nature to cause specific risks with regard to data protection. In this case, specific risks may result from the storage of important amount of personal data. More stored data mean more risks. Naturally, the risk is greater in the presence of sensitive data.

b. The extraordinary capacities of HealthGRID technologies to process huge amount of personal data widely disseminated may also open the door to specific risks with regard to data protection. More operations upon personal data mean more risks. Again, the risk is greater in the case of sensitive data.

c. The size of the HealthGRID information system has to be considered, including its inscription in a broad European or international network: the larger, the riskier.

d. A specific risk could result from the data subjects' instrumentalization as they could appear more as informational sources than as patients. It could also lead to discriminations in the provision of healthcare or medicines or treatment or diagnosis.

e. The duration of the HealthGRID information system could also create specific risks to data protection (the "eternity effect").

f. The use of HealthGRID technologies by public authorities or bodies should be considered as inducing specific risks towards data protection.

g. If the exercise of data subjects' rights is more difficult due to the use of HealthGRID technologies, it should be recognized as a specific risk to data protection.

h. Generally, the use of GRID technologies implies the transfer of personal data outside Europe. The complexity of this kind of information system could lead to acknowledge the presence of specific risks towards data protection.

These criteria may naturally be combined, increasing therefore the risks for data subjects' rights and freedoms.

When considering the specific risks that may occur with the introduction of HealthGRID technologies in healthcare, one should not forget to take into account the benefits of its use. Again, it must be stressed that the new information and communication technologies could help to address these issues.

CONCLUSIONS

The risk management in the processing of personal data is deployed in four steps. Firstly, risks are assessed regarding the purposes of the data processing and not regarding the informational content of the processed personal data. Secondly, this principle is slightly though not completely different for sensitive data. For them, risks are assessed regarding their informational content as well as the purposes of their processing. Thirdly, data processing presenting specific risks for data subjects' rights and freedoms must be subject to a prior checking beforehand. The checking may take place in four different ways. Fourthly, transfers of personal data outside Europe are ruled by special rules. Due to some of its characteristics, the use of HealthGRID technologies in healthcare could induce specific risks with regard to data protection. This issue should be carefully monitored by the data controller as well as by the national supervisory authorities. In these situations, it seems more than appropriate to appoint a personal data protection official, to the benefit of everyone in terms of legitimacy, transparency, data subjects' rights and freedoms, confidentiality, security and efficiency. Finally, the presence of these specific risks should not prevent the use of Grid Technologies in Healthcare notably due to their potential but extraordinary benefits for knowledge and healthcare. It should only induce the adoption of

appropriate measures as previously described in order to ensure the respect of data subjects' rights and freedoms to which the entire HealthGrid Community is deeply committed.

Endnotes

[1] For a first overview on these legal issues : J. HERVEG & Y. POULLET, "HealthGRID from a Legal Point of View", in *From GRID to HEALTHGRID*, IOS Publications, Studies in Health Technology and Informatics, 2005, vol. 115, part 5, pp. 312-218.
[2] Journal officiel des Communautés européennes, n° L 281, 23 Nov. 1995, pp. 31 –50. For an in-depth analysis of the Directive : Y. Poullet, M.-H. Boulanger, C. de Terwangne, Th. Leonard, S. Louveaux & D. Moreau, « La protection des données à caractère personnel en droit communautaire », *Journal des Tribunaux de droit européen*, Brussels, Larcier, 1997, p. 121 et s. (in three parts).
[3] Directive 95/46/EC, Recitals 3, 5, 6, 7, and 9.
[4] Directive 95/46/EC, Recitals 2, 3, 10 and 11.
[5] Directive 95/46/EC, Recital 8. See also art. 1 and Recital 9.
[6] Like Public Order.
[7] On Directive 95/46/EC scope : C.J.C.E., 20 May 2003, Rechnungshof & al., C-465/00, C-138/01 and C-139/01 ; C.J.C.E., 6 Nov. 2003, Bodil Lindqvist, case C-101/01, C. de TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *Revue du droit des technologies de l'information*, Brussels, Ed. Bruylant, 2004, pp. 67-99.
[8] "Processing of personal data" ('processing') means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (Directive 95/46/EC, art. 2.b) (cf. Recital 14).
[9] "Personal data" mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Directive 95/46/EC, art. 2.a).
[10] Directive précitée, art. 3.1.
[11] Directive 95/46/EC, art. 3.2 (cf. Recital 12).
[12] J. HERVEG, "La gestion des risques spécifiques aux traitements de données médicales en droit européen », in *Systèmes de santé et circulation de l'information, Encadrement éthique et juridique*, Paris, Dalloz, 2006.
[13] Usually, sensitive data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
[14] Convention n° 108, Report, Recital 43.
[15] Directive 95/46/EC, art. 8.1.
[16] Directive 95/46/EC, Recital 33. Convention n°108 is not so explicit in its article 6.
[17] Directive 95/46/EC, Recital 53.
[18] Directive 95/46/EC, Recital 54.
[19] Directive 95/46/EC, art. 8. On the ban and its exception, see: J. HERVEG, "The Ban on Processing Medical Data in European Law: Consent and Alternative Solutions to Legitimate Processing of Medical Data in HealthGrid", in *Challenges and Opportunities of HealthGrids*, IOS Press, Amsterdam, Studies in Health Technology and Informatics, vol. 120, 2006, pp. 107-116.
[20] Y. POULLET, M.-H. BOULANGER, C. de TERWANGNE, Th. LEONARD, S. LOUVEAUX, & D. MOREAU, o.c., *Journal des Tribunaux de Droit Européen*, Brussels, Larcier, 1997, p. 152, n° 62.
[21] For example, a commercial company processing medical or genetic data.
[22] Directive 95/46/EC, art. 20.1.
[23] Directive 95/46/EC, art. 20.2.
[24] Directive 95/46/EC, Recital 54.
[25] Directive 95/46/EC, art. 20.3.
[26] The personal data protection official is a person appointed by the data controller in compliance with the national law which governs him. This official is responsible in particular:
- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive,
- for keeping the register of processing operations carried out by the controller, , containing the items of information referred to in article 21.2,

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations (Directive 95/46/EC, art. 18.2).
The presence of a data protection official allows Member States to provide for the simplification of or the exemption from the notification duty (Directive 95/46/EC, art. 18.2).

Selective Bibliography

- BENNETT, B. (ed.), *e-Health Business and Transactional Law*, Washington, BNA Books, 2002, 734 p.
- BOULANGER, M.-H., de TERWANGNE, C., LEONARD, Th., LOUVEAUX, S., MOREAU, D. & POULLET, Y., « La protection des données à caractère personnel en droit européen », *Journal des Tribunaux de Droit Européen*, Bruxelles, Larcier, 1997, p. 121 et s. (en trois parties)
- CALLENS, S. (ed.), *e-Health and the Law*, The Hague, Kluwer Law International, 2003, 183 p.
- CHABERT-PELTAT, C., « La télémédecine », *Revue Alain Bensoussan – Droit des Technologies Avancées*, Paris, 1999, n° 6/3-4, pp. 117-138.
- Commission nationale de l'informatique et des libertés (CNIL-France), Délibération n° 97-049 du 24 juin 1997 portant avis sur la mise en œuvre à titre expérimental d'un réseau de télémédecine sur Internet entre le Centre hospitalier d'Annecy et certains médecins de ville, *Revue Alain Bensoussan – Droit des Technologies Avancées*, Paris, 1999, n° 6/3-4, pp. 169-172.
- DE BOT, D., *Verwerking van persoongegevens*, Kluwer, 2001.
- de TERWANGNE, C., « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », obs. sous C.J.C.E, arrêt du 6 nov. 2003, Bodil Lindqvist, affaire C-101/01, *Revue du droit des technologies de l'information*, Bruxelles, Ed. Bruylant, 2004, pp. 67-99.
- FLEISHER, L.D. & DECHENE, J.C., *Telemedicine and e-Health Law*, Law Journal Press, 2005.
- HERVEG, J., « HealthGRID from a Legal Point of View », in *From GRID to HEALTHGRID*, IOS Publications, Studies in Health Technology and Informatics, 2005, Volume 112, part 5, pp. 312-318.
- HERVEG, J., "The Ban on Processing Medical Data in European Law: Consent and Alternative Solutions to Legitimate Processing of Medical Data in HealthGrid", in *Challenges and Opportunities of HealthGrids*, IOS Press, Studies in Health Technology and Informatics, 2006, Volume 120, pp. 107-116.
- HERVEG, J. "La gestion des risques spécifiques aux traitements de données médicales en droit européen », in *Systèmes de santé et circulation de l'information, Encadrement éthique et juridique*, Paris, Dalloz, 2006.
- HERVEG, J. & VAN GYSEGHEM, J.-M., "La sous-traitance des données du patient au regard de la directive 95/46", *Lex Electronica*, vol. 9, n° 3, t. 2004, http://www.lex-electronica.org/articles/v9-3/herveg_vangyseghem.htm.
- HERVEG, J., VERHAEGEN, M.-N. & Y. POULLET, « Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé », *Revue de Droit de la Santé*, Kluwer, 2002-2003/2, pp. 56-84.
- HERVEG, J., VAN GYSEGHEM, J.-M. & de TERWANGNE, C., *GRID-enabled medical simulation services and European Law*, Final Report on all the Legal Issues related to Running GRID Medical Services, European Research contract IST-2001-37153-GEMSS, 29 February 2005, 341 p.
- IAKOVIDIS I., WILSON, P., Healy J.-Cl., *E-Health: Current Situation and Examples of Implemented and Beneficial E-Health Applications*, IOS Press, Studies in Health Technology and Informatics, 2004, Volume 100, 249 p.
- KAPLAN, G. & Mc FARQUHAR, E., *e-Health Law Manual*, New-York, Aspen Publishers, 2003.
- MIDDLETON, S.E., HERVEG, J., CRAZZOLARA, F., MARVIN, D. & POULLET, Y., « GEMSS : Security and Privacy for a Medical Grid », Stuttgart, Schattaeur, Verlag für Medizin und Naturwissenschaften, *Methods of Information in Medicine*, 2005, 44/2, p. 182-185.
- RIENHOFF, O., LASKE, C., VAN EECKE, P., WENZLAFF, P. & PICCOLO, U., *A Legal Framework for Security in European Health Care Telematics*, Amsterdam, IOS Press, Studies in Health Technology and Informatics, 2000, vol. 74, 202 p.
- RIGAUX, Fr., *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Paris, Bruylant, L.G.D.J., 1990.
- RODRIGUES, R.J., WILSON, P. & SCHANZ, S.J., *The Regulation of Privacy and Data Protection in the Use of Electronic Health Information, An International Perspective and Reference Source on*

Regulatory and Legal Issues Related to Person-Identifiable Health Databases, Pan American Health Information, World Health Organization, 2001, 217 p.

- ROGER-FRANCE, Fr., « Informations de santé, télématique et télémédecine, Perspectives d'ensemble à l'horizon 2000 », *Journal de réflexion sur l'informatique*, 1994, n° 30, pp. 7-9.
- ROUSSEAU, A. & HERVEG, J., *Manuel d'informatisation des urgences hospitalières*, Louvain-la-Neuve, Presses Universitaires de Louvain, 2003, 183 p.
- SILBER, D., *The case for eHealth*, Maastricht, Institut Européen d'Administration Publique (ed.), 2003, 32 p.
- STANBERRY, B., *The Legal and Ethical Aspects of Telemedicine*, London, Royal Society of Medicine Press, 1998, 172 p.
- VAN EECKE, P., "Electronic Health Care Services and the e-Commerce Directive", in *A decade of research @ the crossroads of law and ICT*, Gent, Larcier, 2001, pp. 365-379.
- VILCHES ARMESTO, L., « IMS Health : dernier développement de la C.J.C.E. relatif au refus de licence en droit de propriété intellectuelle », note sous C.J.C.E., 29 avril 2004, Brussels, Larcier, *Revue du Droit des Technologies de l'Information*, 2004, n° 20, p. 59 et s.
- WILSON, P., LEITNER, Chr. & MOUSSALI, A., *Mapping the Potential of eHealth, Empowering the citizen through eHealth tools and services*, Maastricht, European Institute of Public Administration (ed.), 2004, 52 p.